



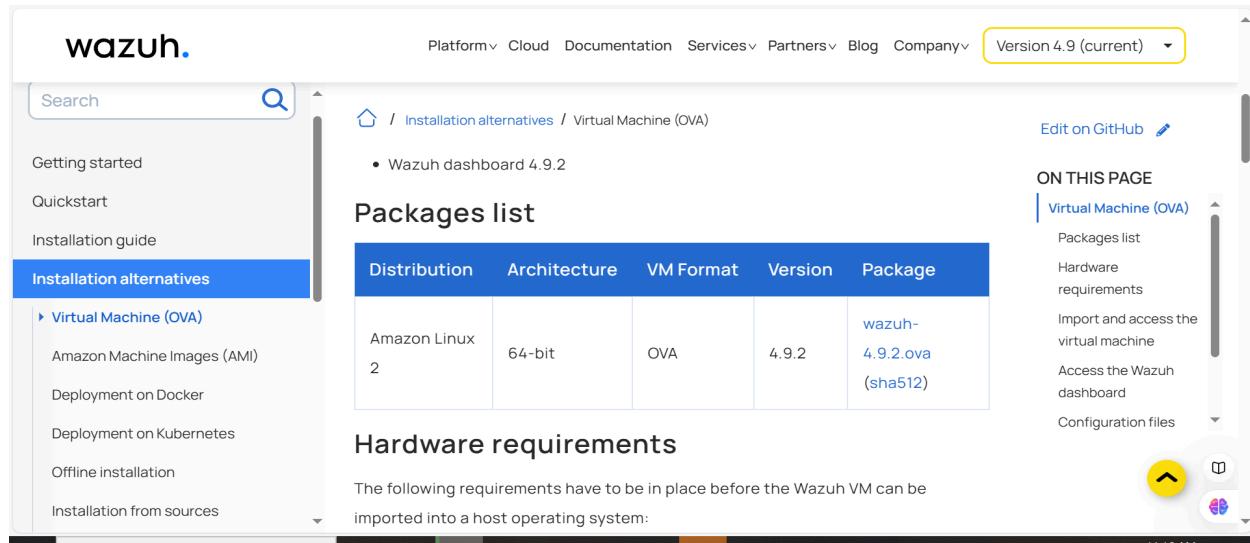
Installing **Wazuh** and Wazuh **Agents**

Sameer Hassan

Linkedin Profile: [Sameer Hassan](#)
Step-by-Step Guide.

*If you need any help during the Process you can
message me I will help you to fix*

1- Downloading.OVA file to Install Wazuh in Window Operating System



The screenshot shows the Wazuh website's 'Virtual Machine (OVA)' page. The top navigation bar includes links for Platform, Cloud, Documentation, Services, Partners, Blog, Company, and a dropdown for 'Version 4.9 (current)'. The left sidebar has sections for Getting started, Quickstart, Installation guide, and Installation alternatives, with 'Virtual Machine (OVA)' selected. The main content area displays a 'Packages list' table with columns: Distribution, Architecture, VM Format, Version, and Package. One row is shown for Amazon Linux 2, 64-bit, OVA format, version 4.9.2, and the package name 'wazuh-4.9.2.ova (sha512)'. Below the table, a section titled 'Hardware requirements' lists prerequisites for importing the VM.

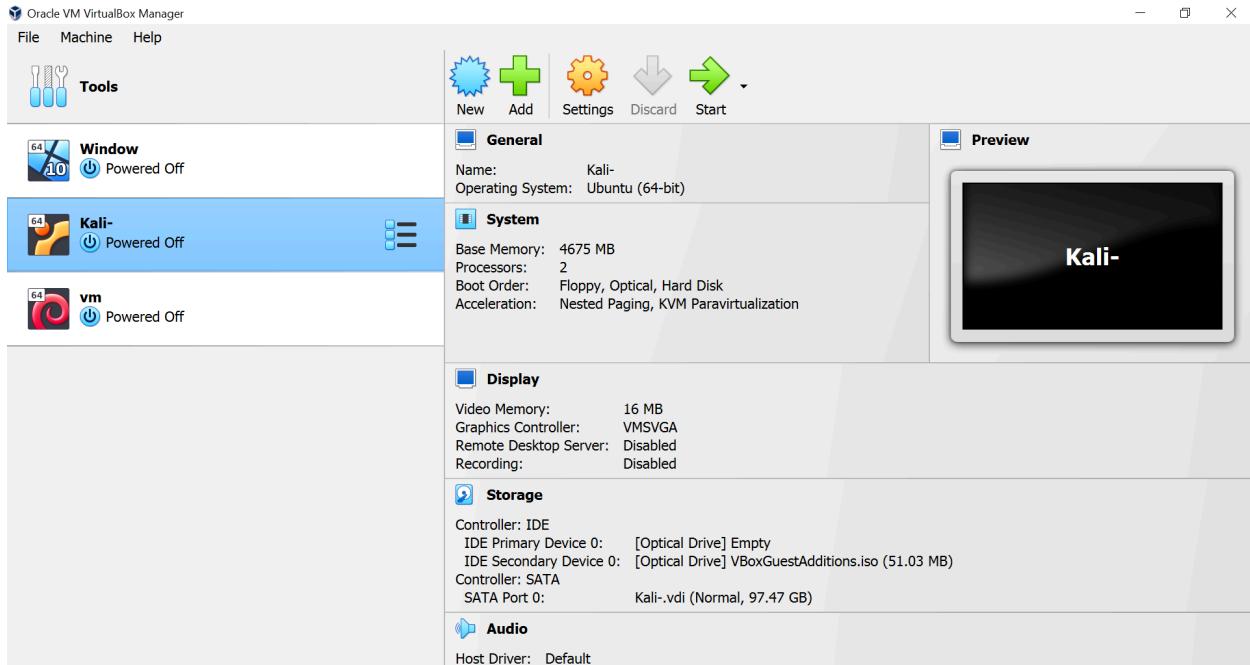
Distribution	Architecture	VM Format	Version	Package
Amazon Linux 2	64-bit	OVA	4.9.2	wazuh-4.9.2.ova (sha512)

The Packages List tells us about the Version File format and Distribution of the Wazuh Current version

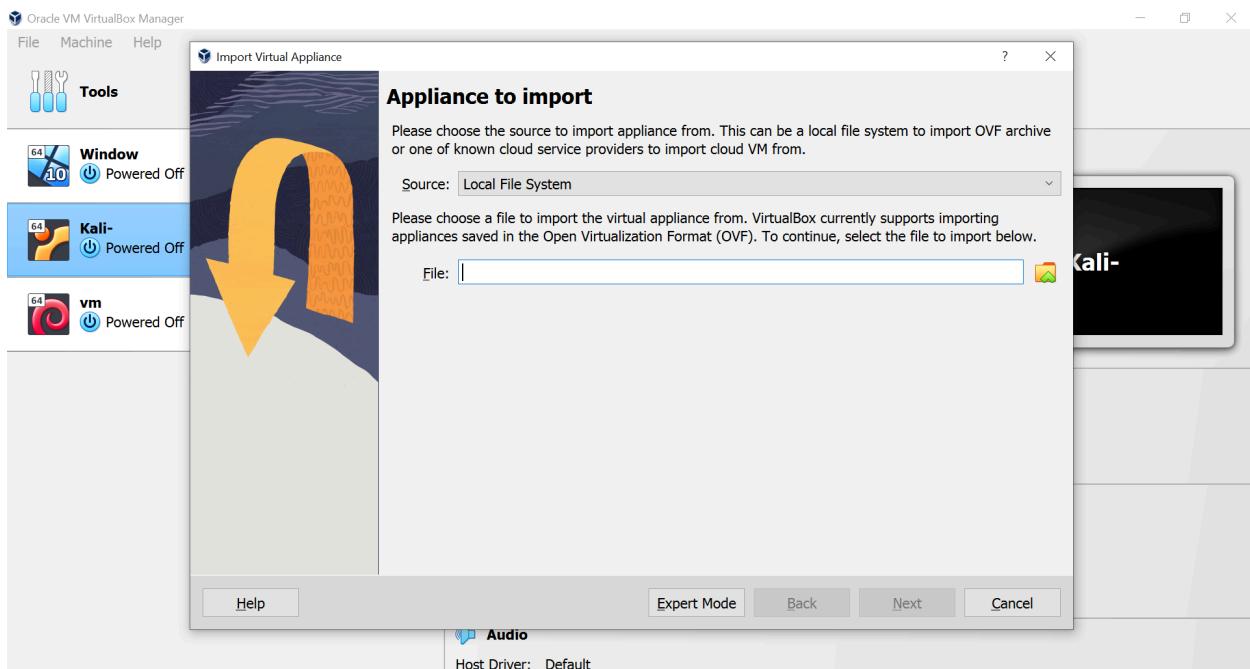
Packages list

Distribution	Architecture	VM Format	Version	Package
Amazon Linux 2	64-bit	OVA	4.9.2	wazuh-4.9.2.ova (sha512)

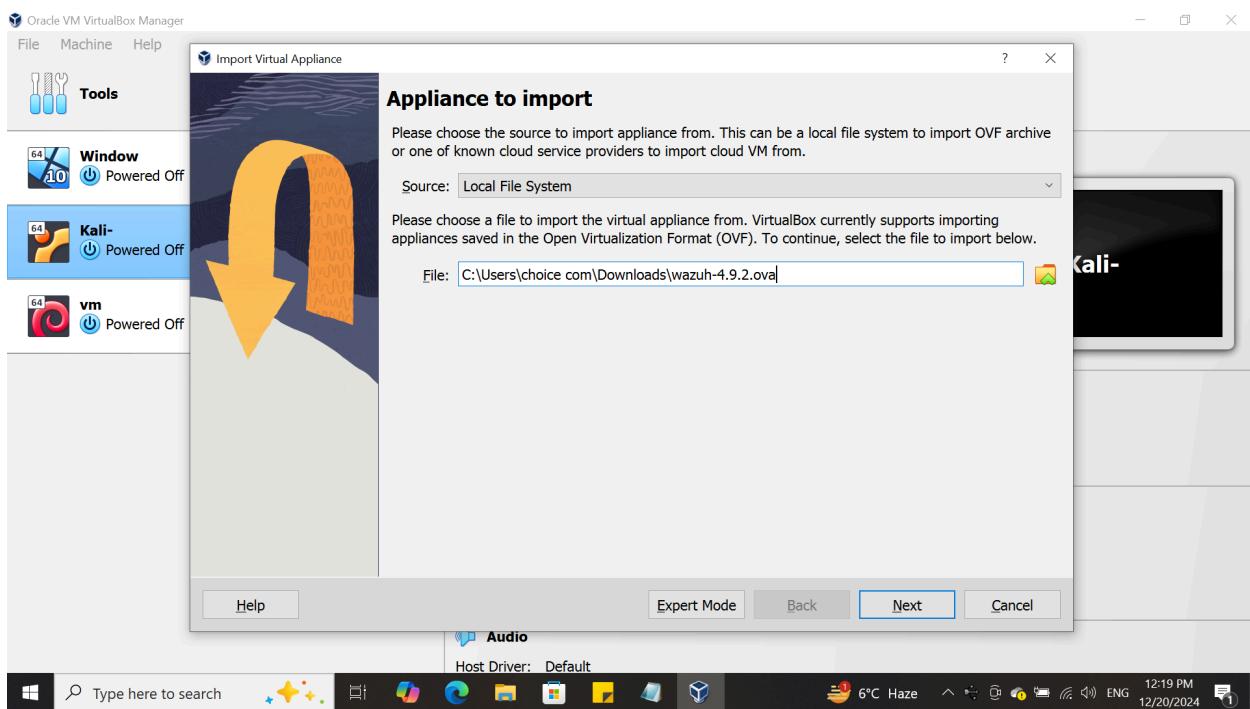
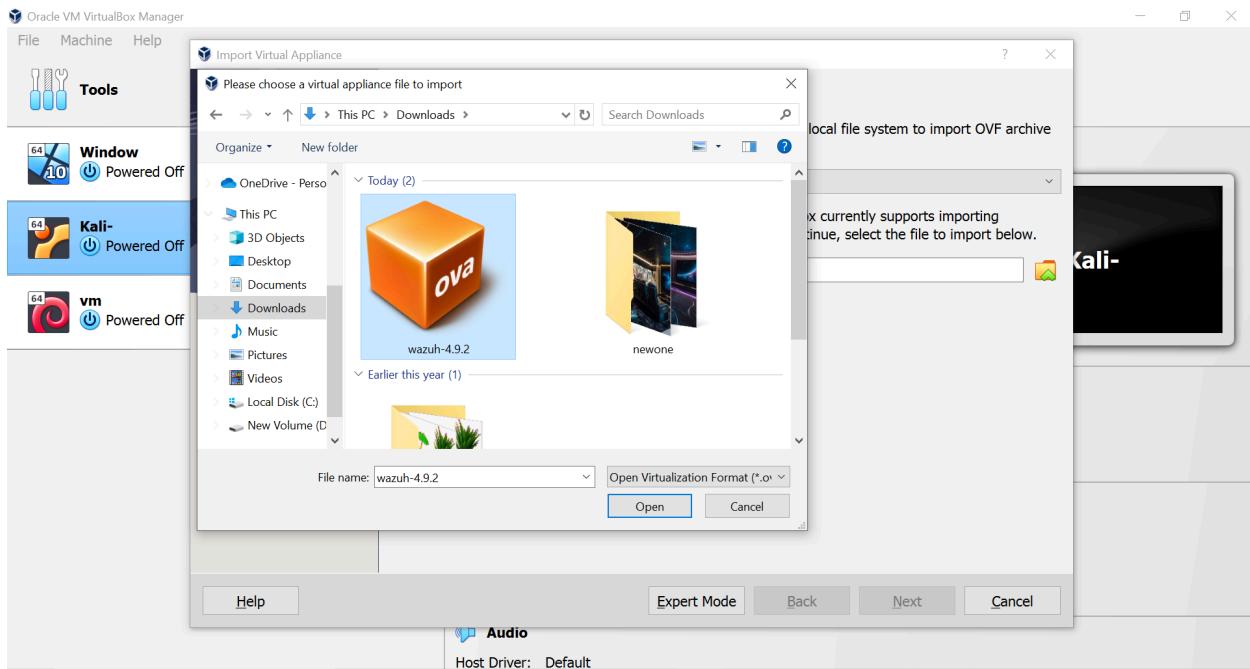
2- Importing the Wazuh OVA file in the Virtual Box.



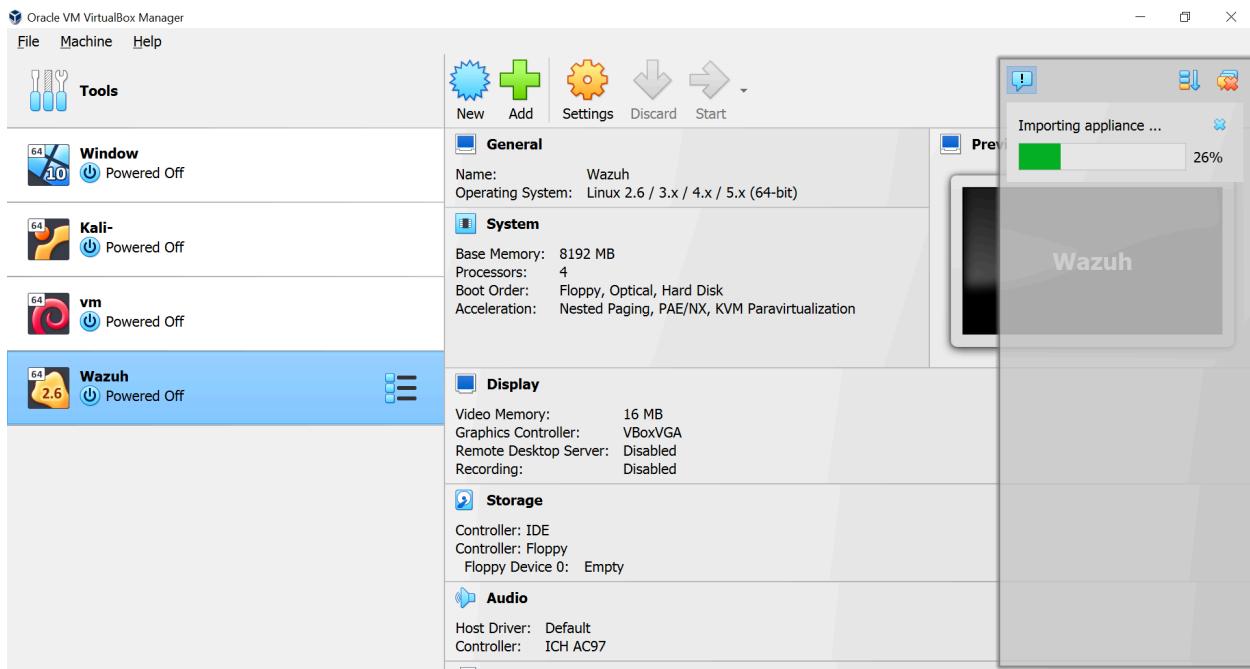
After opening the Virtual Box go to File> Then Import Appliances



Now Select the Ova Wazuh File.



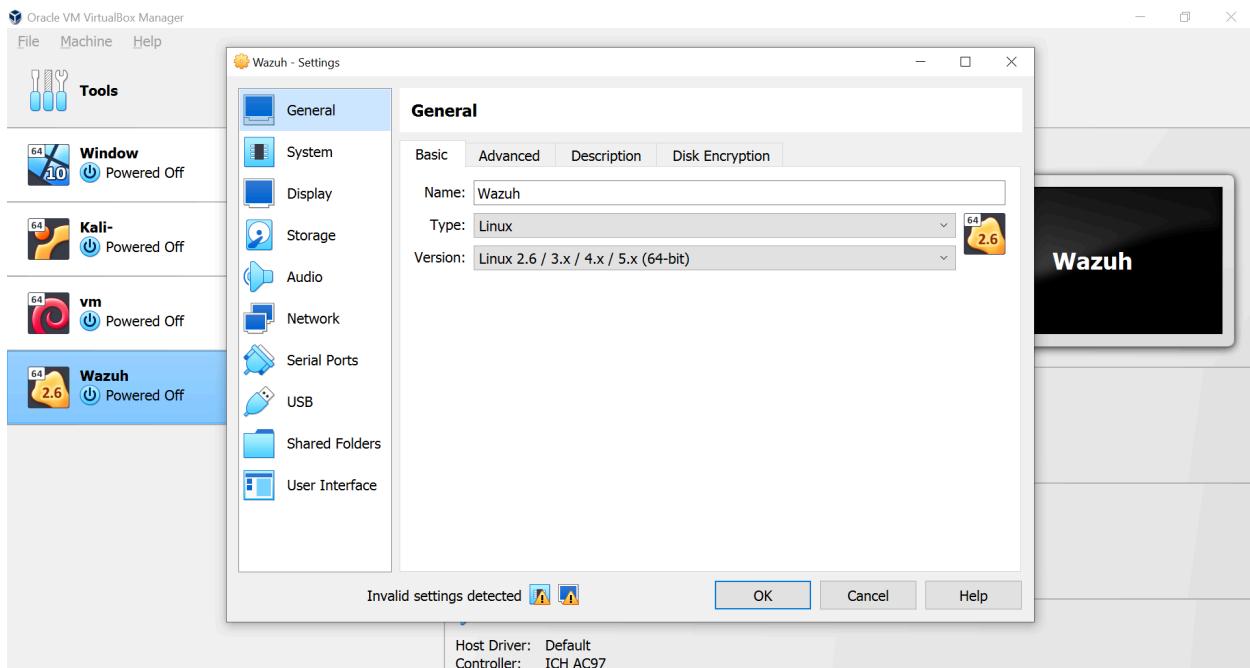
After selecting OVA File Now click on the Next button and then click on Finish Button



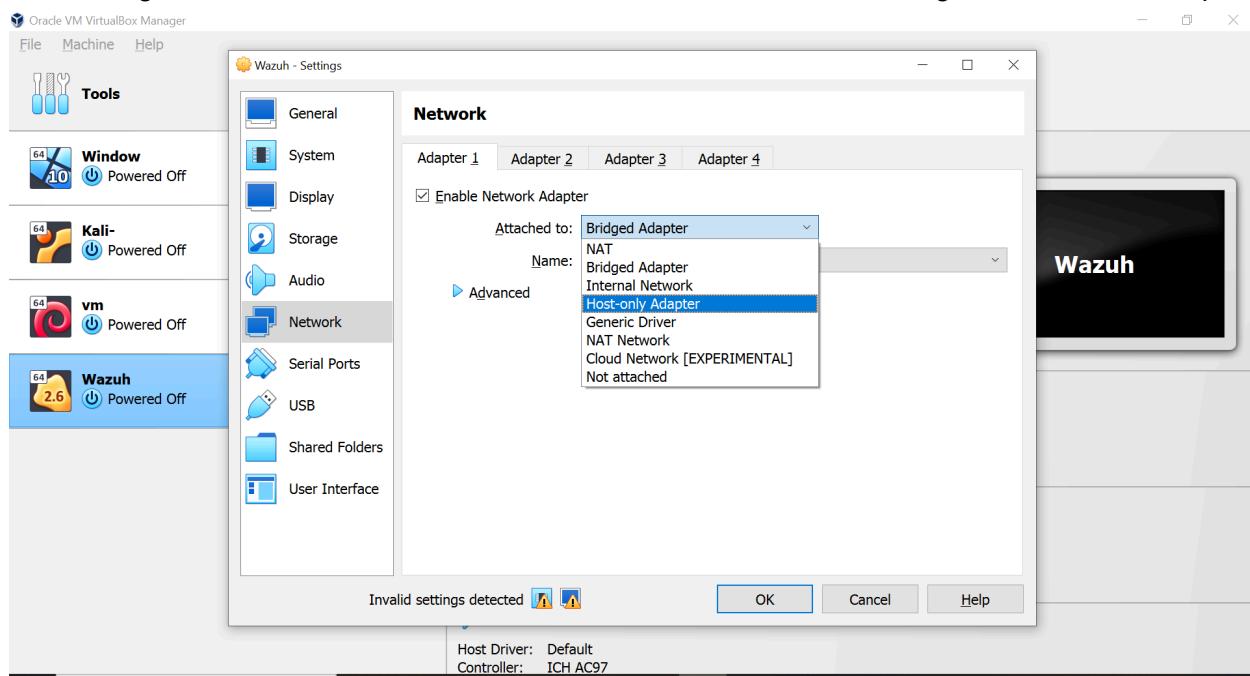
Wazuh File Imported Successfully.

2- Changing the Network Setting to “Host-only Adapter”

Select the Wazuh machine and then Click on the Setting icon



Now go to the Network tab and change the adapter



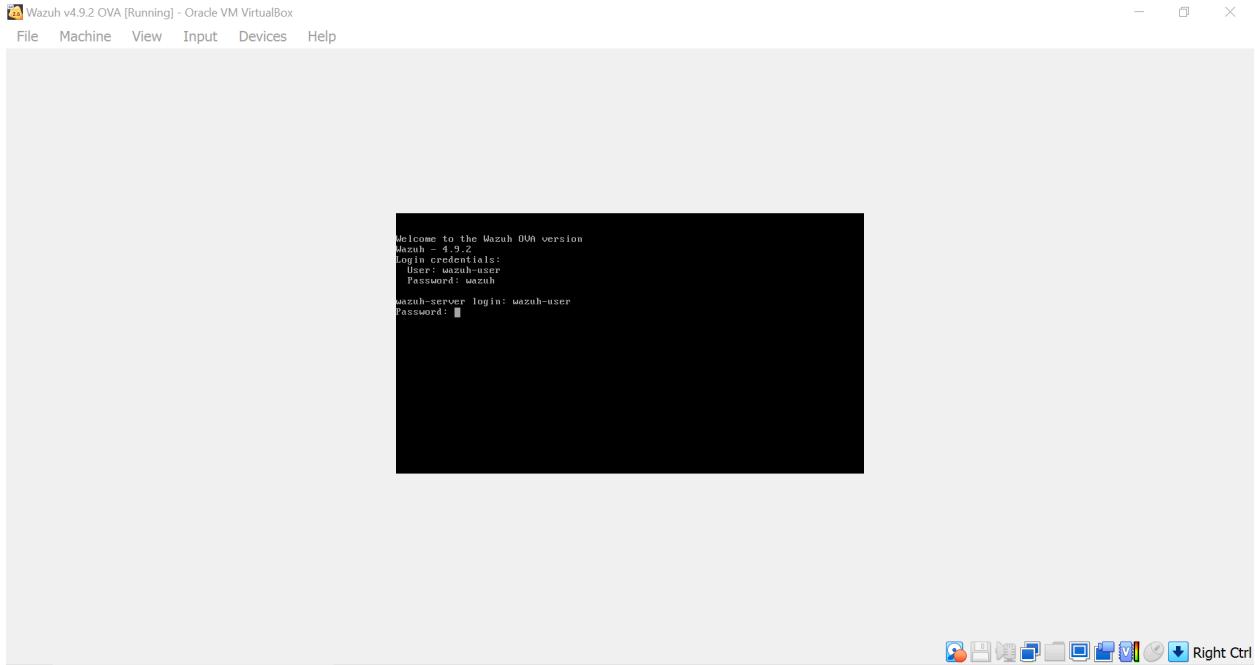
Select Host Only Adapter then Hit OK.

3- Starting the Machine.

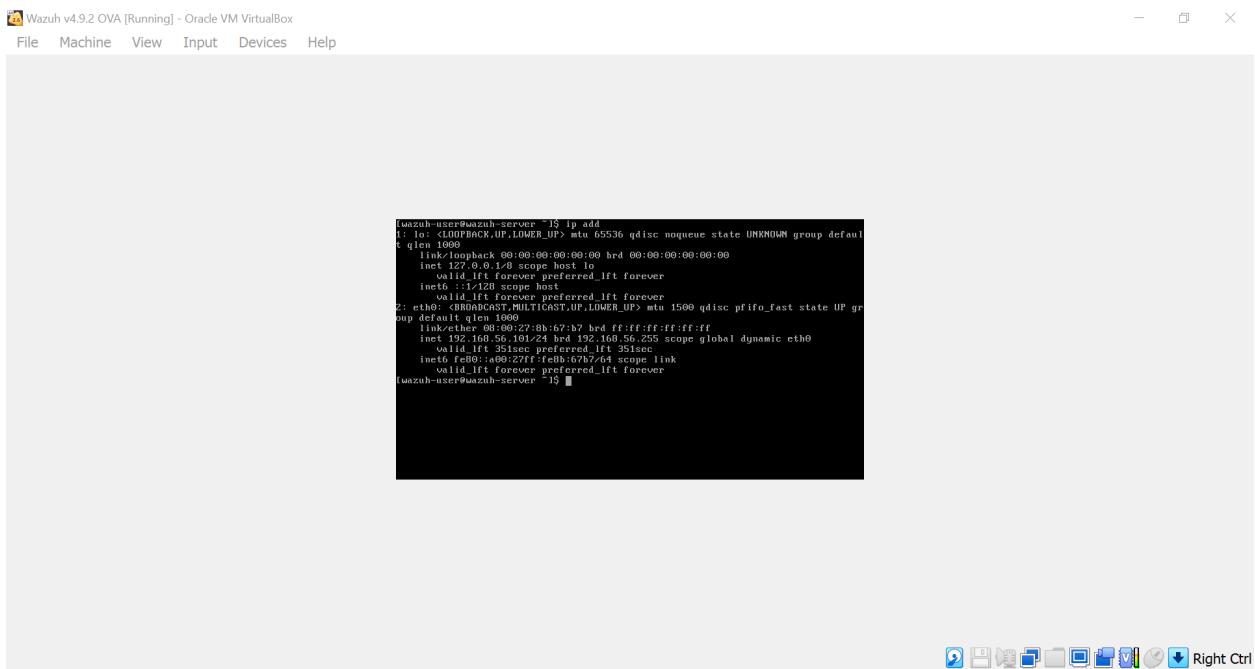
Click on the start button to start the Wazuh. After stating Enter the Username and Password

Username → **wazuh-user**

Password → **wazuh**



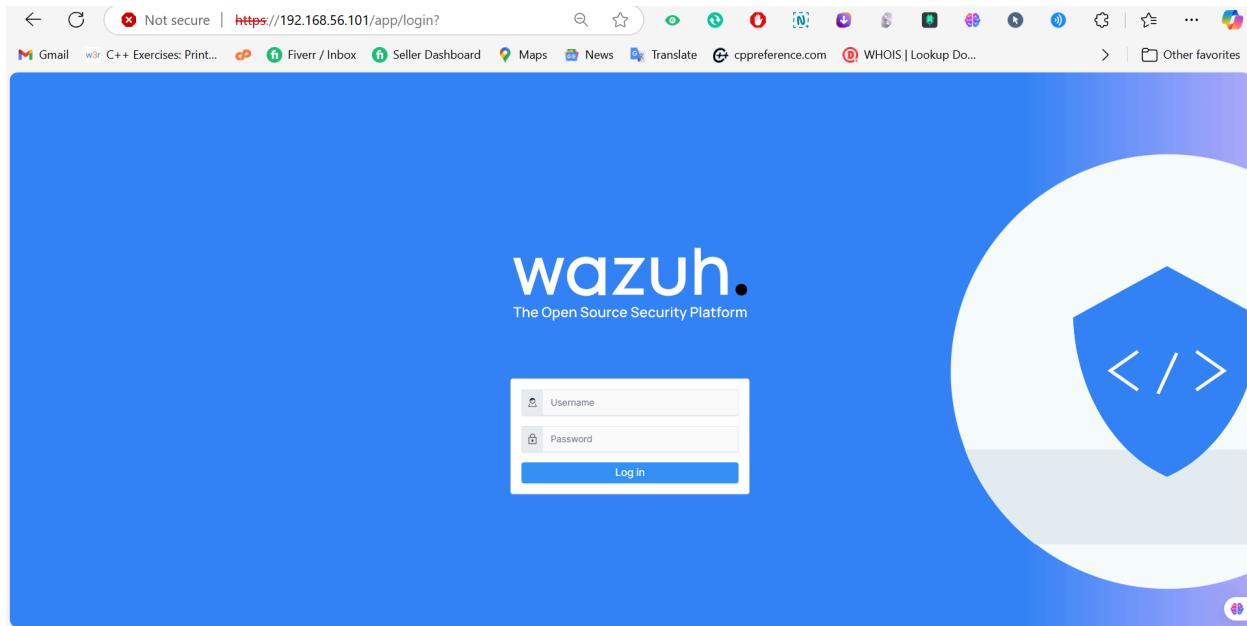
Enter username and Password and then press enter. After login write IP add to check the IP address of your Wazuh machine



My Wazuh IP address is **192.168.56.101**

4- Accessing Wazuh Dashboard.

My Wazuh IP is 192.168.56.101. Type this IP in your browser to access the Wazuh Dashboard.



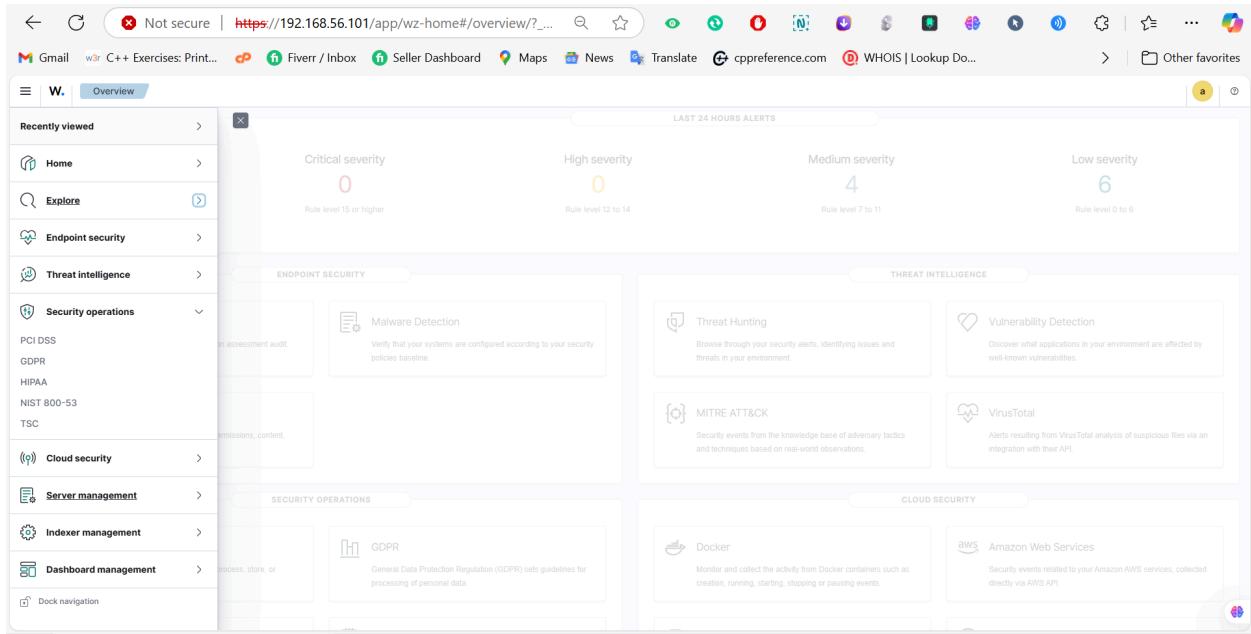
To login to wazuh Dashboard Enter Username and password

Username → **admin**

Password → **admin.**

A screenshot of the Wazuh dashboard. The top navigation bar shows the URL https://192.168.56.101/app/wz-home#/overview/?.... The dashboard is divided into several sections: "AGENTS SUMMARY" (No results), "LAST 24 HOURS ALERTS" (0 Critical, 0 High, 4 Medium, 5 Low), "ENDPOINT SECURITY" (Configuration Assessment, Malware Detection, File Integrity Monitoring), "THREAT INTELLIGENCE" (Threat Hunting, Vulnerability Detection, MITRE ATT&CK, VirusTotal), "SECURITY OPERATIONS" (PCI DSS, GDPR), and "CLOUD SECURITY" (Docker, Amazon Web Services). Each section contains detailed sub-information and icons.

5- Navigating the Dashboard.



6- Deploying Wazuh Agent.

Linux:

Add the Wazuh Repository:

- Open the terminal.
- Add the Wazuh repository by running:

Copy and paste this Command:

```
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo apt-key add -
```

```
echo "deb https://packages.wazuh.com/4.x/apt/ stable main" | sudo tee /etc/apt/sources.list.d/wazuh.list
```



```
Kali- [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(talib@talib) ~
$ curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo apt-key add -
echo "deb https://packages.wazuh.com/4.x/apt/ stable main" | sudo tee /etc/apt/sources.list.d/wazuh.list
[sudo] password for talib:
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
OK
deb https://packages.wazuh.com/4.x/apt/ stable main
(talib@talib) ~
```



Update your Package → **sudo apt-get update**

→ **Install the Wazuh Agent:**

Run the following command to install the Wazuh agent → **sudo apt-get install wazuh-agent**



```
Kali- [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(talib@talib) ~
$ curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo apt-key add -
echo "deb https://packages.wazuh.com/4.x/apt/ stable main" | sudo tee /etc/apt/sources.list.d/wazuh.list
[sudo] password for talib:
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
OK
deb https://packages.wazuh.com/4.x/apt/ stable main
(talib@talib) ~
$ sudo apt-get update
Get:1 https://packages.wazuh.com/4.x/apt stable InRelease [17.3 kB]
Get:2 https://packages.wazuh.com/4.x/apt stable/main amd64 Packages [41.6 kB]
Get:3 https://mirrot.math.princeton.edu/pub/kali kali-rolling InRelease [41.5 kB]
Get:4 https://mirrot.math.princeton.edu/pub/kali kali-rolling/main amd64 Packages [20.3 kB]
Get:5 https://mirrot.math.princeton.edu/pub/kali kali-rolling/main amd64 Contents [deb] [48.9 kB]
Get:6 https://mirrot.math.princeton.edu/pub/kali kali-rolling/contrib amd64 Packages [110 kB]
Get:7 https://mirrot.math.princeton.edu/pub/kali kali-rolling/contrib amd64 Contents [deb] [260 kB]
Get:8 https://mirrot.math.princeton.edu/pub/kali kali-rolling/non-free amd64 Packages [194 kB]
Get:9 https://mirrot.math.princeton.edu/pub/kali kali-rolling/non-free amd64 Contents [deb] [877 kB]
Fetched 722 kB in 4min 44s (256 kB/s)
Reading package lists...
W: https://packages.wazuh.com/4.x/apt/dists/stable/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.
N: Repository 'Kali Linux' changed its 'non-free component' value from 'non-free' to 'non-free non-free-firmware'
N: More information about this can be found online at: https://www.kali.org/blog/non-free-firmware-transition/
(talib@talib) ~
$ sudo apt-get install wazuh-agent
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  wazuh-agent
0 upgraded, 1 newly installed, 0 to remove and 2044 not upgraded.
Need to get 10.8 MB of archives.
After this operation, 39MB of additional disk space will be used.
Get:1 https://packages.wazuh.com/4.x/apt stable/main amd64 wazuh-agent amd64 4.9.2-1 [10.8 MB]
Preconfiguring packages
Selecting previously unselected package wazuh-agent.
(Reading database... 395577 files and directories currently installed.)
Preparing to unpack .../wazuh-agent_4.9.2-1_amd64.deb ...
Unpacking wazuh-agent (4.9.2-1) ...
Setting up wazuh-agent (4.9.2-1) ...

(talib@talib) ~
```



Configure the Wazuh Agent:

- Open the file manager and navigate to /var/ossec/etc/.
- Open the ossec.conf file with a text editor.
- Find the <address> tag and set it to your Wazuh manager's IP address.



Kali- [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

ossec.conf

```
GNU nano 8.0
```

```
<!-- Wazuh - Agent - Default configuration for kali 2024.2
More info at: https://documentation.wazuh.com
Mailing list: https://groups.google.com/forum/#forum/wazuh
-->

<ossec_config>
  <client>
    <server>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config_profile>kali, kali2024, kali2024.2</config_profile>
    <notify_time>10</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
    <crypto_method>aes</crypto_method>
  </client>

  <client_buffer>
    <!-- Agent buffer options -->
    <disabled>no</disabled>
    <queue_size>5000</queue_size>
    <events_per_second>500</events_per_second>
  </client_buffer>

  <!-- Policy monitoring -->
  <rootcheck>
    <disabled>no</disabled>
    <check_files>yes</check_files>
    <check_trojans>yes</check_trojans>
    <check_syscalls>yes</check_syscalls>
    <check_pids>yes</check_pids>
    <check_ports>yes</check_ports>
    <check_if>yes</check_if>
  </rootcheck>
  <!-- Frequency that rootcheck is executed - every 12 hours -->
  <frequency>3200</frequency>
  <rootkit_files>etc/shared/rootkit_files.txt</rootkit_files>
  <rootkit_trojans>etc/shared/rootkit_trojans.txt</rootkit_trojans>
  <skip_nfs>yes</skip_nfs>
```

Help Exit Write Out Read File Where Is Cut Paste Execute Justify Location Go To Line M-U Undo M-D Redo A Set Mark To Bracket Previous Next Back Forward Prev Word Next Word Home End Right Ctrl

After adding ip save it and start the agent. **sudo systemctl start wazuh-agent**



Kali- [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

talib@talib: ~

```
$ sudo systemctl status wazuh-agent
```

[sudo] password for talib:

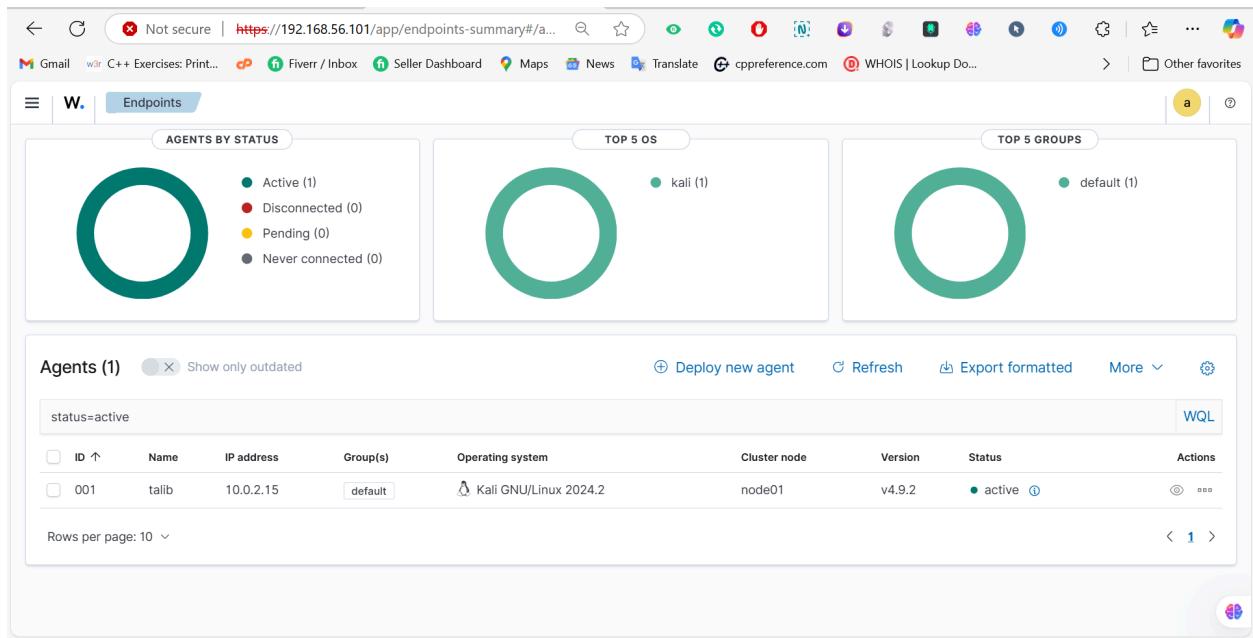
```
wazuh-agent.service - Wazuh agent
  Loaded: loaded (/usr/lib/systemd/system/wazuh-agent.service; disabled; preset: disabled)
  Active: active (running) since Sat 2024-12-21 09:15:05 EST; 1min ago
    Process: 30768 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
   Tasks: 32 (limit: 5280)
  Memory: 5G (4G max; 1.2G)
     CPU: 51.235s
    CGroup: /system.slice/wazuh-agent.service
            └─1181 /var/ossec/bin/wazuh-execd
              ├─1182 /var/ossec/bin/wazuh-sysmond
              ├─1211 /var/ossec/bin/wazuh-syscheckd
              ├─1233 /var/ossec/bin/wazuh-logcollector
              └─1258 /var/ossec/bin/wazuh-moduled
```

```
Dec 21 09:15:00 talib systemd[1]: Starting wazuh-agent.service - Wazuh agent...
Dec 21 09:15:00 talib env[30768]: Starting Wazuh v4.9.2...
Dec 21 09:15:01 talib env[30768]: Started wazuh-agent...
Dec 21 09:15:01 talib env[30768]: Started wazuh-syscheckd...
Dec 21 09:15:01 talib env[30768]: Started wazuh-logcollector...
Dec 21 09:15:01 talib env[30768]: Started wazuh-moduled...
Dec 21 09:15:05 talib env[30768]: Completed
Dec 21 09:15:05 talib systemd[1]: Started wazuh-agent.service - Wazuh agent.
```

talib@talib: ~

7- Verification.

Agent Installed Successfully.



8-Summary.

Successfully installed and configured the Wazuh manager and deployed agents on Ubuntu.

Linkdin profile <https://www.linkedin.com/in/sameer-hassan-15a428255/>